MODELO DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN, AMENAZAS A LA PRIVACIDAD Y PROTECCIÓN DE LOS DATOS EN INTERNET DENTRO DE LA ADMINISTRACIÓN DE JUSTICIA EN LA GESTIÓN TECNOLÓGICA.

Niño Cifuentes Eliana
elikero@yahoo.es
Universidad Piloto de Colombia

Abstract**—** *Institutions should have certainty that they are subject to risks that affect their operational role and the right knowledge of them guarantees continued productivity over time.*

A risk must be understood as an external or internal agent, exposing to danger the organization. There are many types of risks, even so, whichever the risk class is, if an entity not faces that danger in the shortest possible time, increases in an exponentially sense the deterioration of the image of the organization. In that way, a company and especially its management level must manage risk and establish principles and methodologies able to cope and/or mitigate them, establish risk maps and to establish policies in order to manage risk appropriately. The privacy in the new systems of information storage, such as clouds is an important progress in countries like Colombia, because not only is used by individuals, but also by corporate groups, and even by state entities, such as the Consejo Superior de la Judicatura, facilitating the proper administration of justice. However, the security issues set out in this document, they do seem like a vulnerable system, but to follow the instructions presented here, we ensure safe handling of the information stored in nonphysical data bases.

Keywords**—** *Risk, security, organization, cloud, protection, information, passwords, encryption, double authentication, vulnerability and controls.*

Resumen**—** *Las entidades deben tener certeza que están sujetas a riesgos que afectan su función operativa y el debido conocimiento de los mismos les garantiza productividad continuada en el tiempo.*

Un riesgo debe ser entendido como un agente externo o interno, que expone al peligro a la organización. Existen muchas clases de riesgos, sin embargo, sea cual sea la clase de riesgo, si una entidad no afronta en el menor tiempo posible dicho peligro, aumenta en sentido exponencial el deterioro de la imagen de la organización. Así las cosas, en una empresa y en especial su nivel directivo deben gestionar los riesgos y establecer principios y metodologías capaces de afrontarlos y/o mitigarlos, establecer mapas de riesgo y establecer políticas con el fin de administrar el riesgo de forma adecuada. La privacidad en los nuevos sistemas de almacenamiento de información, como las nubes es un avance importante en países como Colombia, pues no sólo es usada por particulares, sino también por grupos corporativos, e incluso, por entidades estatales, como es el caso del Consejo Superior de la Judicatura, facilitando la correcta administración de justicia. Sin embargo, los problemas de seguridad que se exponen en este documento, lo hacen parecer un sistema vulnerable, pero al seguir las recomendaciones también aquí expuestas, aseguramos un manejo seguro de la información almacenada en bases de datos no físicas.

Índice de Términos**—** *Riesgo, seguridad, organización, nube, protección, información, contraseñas, cifrado, doble autenticación, vulnerabilidad y controles.*

I. INTRODUCCIÓN

Antes de comenzar es preciso definir que el riesgo (dentro de este modelo de gestión) es todo aquel suceso que pueda poner en peligro el procedimiento o tenga impacto sobre los objetivos institucionales, y en ese orden de ideas, la existencia misma de la organización. Entendido éste dentro de una organización pública, el riesgo toma una vital importancia, pues está sujeto a control por la organización, para que los objetivos de la misma sean cumplidos.

La cultura de prevenir o minimizar algunos eventos que no permitan la correcta aplicación del Modelo de Administración de Riesgos (MAR), recae directamente en los titulares de los procesos de riesgos.

Se pueden tener en cuenta algunos de los siguientes parámetros para el mejoramiento de la gestión administrativa de riesgos.

- Enfocar exclusivamente los riesgos relevantes y sus controles internos correspondientes.
- Correlacionar los factores, efectos o causas que corresponden a más de un riesgo, los cuales no necesariamente pertenecen a un mismo proceso, procedimiento, área, etc., y que al materializarse como riesgos, impactan en la gestión de la institución.
- Lograr una adecuada priorización de los objetivos institucionales.
- Ejercer una evaluación sobre el grado de cumplimiento de las metas u objetivos institucionales.
- Conocer los nuevos eventos que pongan en riesgo el cumplimiento de las tareas institucionales previstas.

La administración debe estar orientada en procedimientos sencillos y bien dirigidos, evitando en todo caso en incurrir en costos excesivos que sobrepasen los beneficios esperados.

Cada dependencia, o titular de área dentro de la organización, deberá tomar las precauciones y recomendaciones necesarias para disminuir y/o prevenir el riesgo en la mayor medida posible.

El riesgo se mide en términos del grado de impacto y probabilidad de ocurrencia en la organización, el primero mide la dureza del resultado cuando el riesgo ocurra; el segundo, se refiere a la posibilidad de que se presente o no un evento riesgoso. Así mismo, estos riesgos deben ser sub organizados en una matriz diferente, tomando en cuenta su *causa* (situación existente, hecho o certidumbre que puede resultar riesgosa), *su efecto* (resultado probable) y *el factor de riesgo* (características observables que indican la presencia de un riesgo o el probable aumento de éste).

La privacidad en internet, es un elemento que últimamente se ha tornado de uso mayormente personal, pues es en principio creado para los usuarios tomados como individuos quienes pueden ofrecer información vulnerable en internet y para quienes se han creado específicamente ciertas políticas y normas de privacidad en internet. A pesar de esto, el ámbito corporativo también saca provecho de los beneficios que el internet puede ofrecer, pero es en este caso en donde se debe hacer mayor énfasis en cuanto a la protección y la privacidad de los datos corporativos, por cuanto estos son objeto de ataques en un mayor grado.

Así pues, la privacidad en internet en el mundo corporativo, no puede ser de ningún modo un tema tomado a la ligera, más cuando se trata de información que respecta a vulnerabilidades propias de una empresa. Teniendo en cuenta esto, toda precaución es mínima y ante la evolución del almacenamiento de datos de la manera más segura posible, resalta entre muchas opciones “la nube”, un sistema que permite almacenar la información en la misma internet, sin el uso de elementos físicos y a la cual se puede acceder desde casi cualquier lugar que posea una conexión a internet; la practicidad y eficiencia de esta herramienta para el almacenamiento de datos, ofrece una gran cantidad de ventajas, pero así mismo, un gran número de puntos vulnerables para las empresas que usan este sistema si no toman la precauciones de proteger lo que suben a internet.

II. PRINCIPALES RIESGOS EN LA ADMINISTRACIÓN DE JUSTICIA EN LA GESTIÓN TECNOLÓGICA

El mapa de riesgos dentro de una organización, en el caso concreto el Consejo Superior de la Judicatura, presenta elementos claves para la identificación plena de un riesgo probable, y en caso que éste se ejecute, se minimicen sus efectos en la organización. Así pues, encontramos la identificación del riesgo y su respectiva descripción, como los hechos concretos que contrarían los objetivos de la gestión tecnológica. A continuación se realiza una valoración de la probabilidad e impacto preliminares de cada riesgo evaluado, lo que deviene en una evaluación conjunta y les son adjudicados valores de relevancia (tolerante, aceptable, importante o moderado, y según el caso, clasificados en niveles numéricos 1 y 2). Es entonces cuando se evalúan los controles existentes para disminuir o soslayar ese riesgo,

teniendo en cuenta que el factor control es el más importante dentro del mapa de riesgos. Así mismo se desprenden preguntas concernientes a su rendimiento, que buscan, la disminución de la probabilidad e impacto del riesgo. Todo esto permite efectuar una tasación acertada del riesgo, tomando en cuenta los anteriores factores y eventos, este trabajo se concluye con la apreciación de opciones de manejo del riesgo, desde una óptica más acertada bajo el mismo estudio previo.

En cuanto a las descripciones de cada uno de los factores de riesgo en la gestión tecnológica del consejo superior de la judicatura, encontramos entre otros, los siguientes:

1. Incumplimiento en los tiempos de respuesta a los usuarios, causado por, fallas en la coordinación y atención de los requerimientos, ocasionando, inconformidad en los usuarios. Problemas que involucran el tiempo de respuesta al usuario, suponen un riesgo importante, con un impacto catastrófico, puesto que ésta afectación retardaría las funciones de cada área, y por ende a toda la organización de administración de justicia.

2. Daños a los sistemas computarizados causado por la desactualización de antivirus o deficientes controles en el acceso a páginas de internet, ocasionando perdida de información y mala imagen institucional. Al igual, que el anterior, éste evento de riesgo supone un retardo en el cabal cumplimiento de funciones externas, de igual modo, éste riesgo representa un valor importante, con un impacto preliminar alto.

3. Degradación en el servicio de telecomunicaciones o disminución de la calidad de conexión a la red telemática de la Entidad, causado por el alta demanda del ancho de banda de la red, ocasionando lentitud del procesamiento de datos y afectando a los usuarios finales.

4. Daños en los componentes físicos de un elemento tecnológico que impiden su correcto funcionamiento causado por defectos de fabricación, accidentes o deterioro por uso. Un riesgo que podría denominarse común, supone un riesgo moderado al funcionamiento de la gestión tecnológica, puesto que si no se realiza un correcto mantenimiento a la estructura que soporta el sistema tecnológico de la organización, ésta eventualmente colapsará.

5. Fallas de software al servicio de la Rama Judicial, causado por degradación de los Sistemas y aplicativos, ocasionando demoras en la gestión de los despachos judiciales. Es allí, en los despachos judiciales, en donde más se necesita la agilidad y eficiencia, lograda por el conjunto de departamentos a su servicio, pues garantiza el oportuno acceso a la justicia para los colombianos.

6. Desactualización de la infraestructura tecnológica causada por la disminución de recursos presupuestales asignados por parte de Planeación Nacional ocasionando incrementar el nivel de obsolescencia en la infraestructura tecnológica de la Rama Judicial.

III. CONTROLES EXISTENTES PARA CADA FACTOR DE RIESGO EN LA ADMINISTRACIÓN DE JUSTICIA EN EL ÁREA DE GESTIÓN TECNOLÓGICA

Según el caso, pueden implementarse medidas de control destinadas a disminuir el impacto de cada evento riesgoso, optimizando así el servicio y funcionalidad del área de gestión tecnológica, mejoramiento que se ve reflejado en los objetivos de la organización, como la pronta y adecuada administración de justicia.

Para los eventos hipotéticos de incumplimiento del servicio a otros departamentos de la organización, o demora en el mismo, se puede implementar la supervisión por parte del ingeniero delegado, ejerciendo control mediante reportes de seguimiento.

Otro evento de riesgo frecuente, relacionado con el daño, falta de mantenimiento u equipo obsoleto, puede ser manejado con medidas como activación de mantenimientos preventivos y/o correctivos, así como también, la exigencia en las garantías de los equipos y en caso de ser muy urgente, realizar atención inmediata por parte de los empleados de sistemas.

Casos relacionados en el deterioro o fallo en la red inalámbrica de internet o la telemática de la misma organización, pueden ser gestionados correctamente mediante control permanente de: la conectividad, activación de alarmas informativas, registro de actividad en la red, Implementación de políticas de navegación, entre otras.

Cuando el evento riesgoso se refiera a la desactualización del equipo, fallas en la estructura, mantenimiento, o deterioro de éste, se controlará mediante un plan de suministro de repuestos bajo demanda, planes de renovación de la infraestructura tecnológica, y una acción de destinación presupuestal para la actualización tecnológica y renovación de equipos.

IV. PÉRDIDA DE PRIVACIDAD Y MECANISMOS PARA PROTEGER LA INFORMACIÓN EN INTERNET

En internet la privacidad es un tema que toma muchos matices, pues es una prioridad en muchos lugares en internet y es objeto de especial protección, pero aun así, somos nosotros mismos quienes tenemos la imperiosa necesidad de hacer público muchos de los acontecimientos que nos ocurren a diario, esta conducta, puede ser leída hoy en día por sistemas integrados, que pueden establecer un patrón de conducta teniendo como base nuestras publicaciones diarias, cosa que presupone un riesgo enorme a nuestra seguridad.

En la esfera de la privacidad de la información, no siempre ocurre lo mismo, pues hay un poco más de conciencia de lo que se está en riesgo si dicha información se vuelve pública, más cuando se trata de la protección de datos empresariales, es allí donde surge el interés por almacenar los datos de una manera más práctica y segura y en la nube parece ser la solución más adecuada. Es por esta razón que merece la pena que la nube sea objeto de una mayor divulgación, acompañada de una implementación adecuada y una educación empresarial acorde a las necesidades de seguridad de la misma.

Las amenazas informáticas, son uno de los principales problemas en el almacenamiento de la información en una nube, pues peligros como el phishing o la vulneración a servidores y contraseñas, ponen a disposición de terceros la información confidencial de la víctima; riesgos como éste y muchos otros se pueden disminuir con conductas como la implementación de antivirus, firewall o un sistema de doble autenticación (éste sistema provee un código de acceso para cierta información restringida que necesita ser verificado también en un dispositivo móvil).

Un riesgo al “colgar” información en la nube es el acceso indebido a la información por parte de terceros, pues si bien ningún sistema está exento de ser vulnerable ante estos ataques, con las precauciones previas necesarias, como el encriptado de la información, se pueden frustrar estos ataques. El sistema de encriptado hace ilegible la información para quienes no otorguen una contraseña previamente establecida, haciendo muy difícil que terceros puedan descifrar dicha información.

V. LOS RETOS DE LA SEGURIDAD EN LA NUBE

Otro aspecto importante a examinar en el sistema de la nube, es el país en el que reside el servidor que almacena la información de la nube, pues cada país tiene un marco normativo que puede ser más o menos estricto según sus propios intereses en el almacenamiento de información. Por supuesto un sistema estricto y eficaz puede favorecer a la protección de datos y por el contrario, un sistema menos riguroso o inexistente puede hacer de la información un blanco fácil para ser vulnerado.

Las legislaciones que tratan este tema, son también una herramienta para los países que quieren garantizar una buena experiencia a los usuarios de

éste servicio de almacenamiento de datos, pues tipificar conductas como los fraudes electrónicos y la violación de la privacidad, ofrece cierta tranquilidad y una garantía de no impunidad a quienes cometan dichos delitos.

Otro tema que merece ser evaluado y que tiene que ver directamente con las legislaciones, esta vez no de países, si no de corporaciones que brindan servicios en el internet, son las políticas de privacidad, pues las redes sociales, como medio de comunicación, exponen mucho de nuestra privacidad a personas de toda índole, es por esto que se han creado medidas como la política de uso de datos o declaración de derechos y responsabilidades, así como también aconsejar a los usuarios de cómo proteger su información de terceros.

VI. CONSEJO SUPERIOR DE LA JUDICATURA Y EL ÁMBITO EMPRESARIAL

Ya que los procesos judiciales pueden ser consultados por cualquiera a través de la página de internet de la CSJ, la vulnerabilidad de este sistema, y aunque solo funcione como sistema de consulta, es muy alta, debido a que con un simple instructivo en una línea de trabajo puede modificar e incluso borrar la información sobre un proceso, debido a estas, palabras reservadas dentro de los 23 caracteres del cuadro de búsqueda, como “Select”, “Delete”, “From”, “Update”; son evaluados y descartados por programas impidiendo que se complete la búsqueda y se eviten acciones dañinas para la Base de Datos.

Otro punto débil en el Consejo Superior de la Judicatura que puede ser objeto de ataques, es la configuración de correos tanto institucionales como particulares. Esta herramienta funciona como un medio de comunicación entre los despachos y las diferentes secciones que componen el CSJ y es por esto mismo que el nivel de información que se maneja en estos correos es de vital importancia para los procesos judiciales manejados por jueces y magistrados. Resulta importante entonces proteger muy bien las contraseñas de estos correos, pues es la principal manera de protegerlos ante eventuales ataques y la suplantación de identidad.

Proteger sistemas, como estos, se vuelve entonces una necesidad urgente, pues garantizar una consulta segura a los ciudadanos que deseen conocer un proceso judicial, es tan importante como el proceso en sí mismo. El correcto acceso a la justicia se ve ejemplificado como una garantía del estado social de derecho y llevado a la realidad en instancias tan aisladas como el acceso a la información judicial puesta a disposición para todos los colombianos en el internet.

Si bien es cierto que la información puesta al servicio de todos en plataformas como la de la página del CSJ es entre otras características, claro, oportuno y verídico, no es ilimitado, pues no es posible acceder a él en su totalidad, ya que esta última característica devendría en un riesgo informático a nivel estatal, poniendo el riesgo el acceso a la justicia.

VII. SUGERENCIAS DE SEGURIDAD EN INTERNET

La privacidad en internet depende principalmente de la prevalencia que le demos a la información que aportamos y que eventualmente pueda llegar a ser publica, pues si bien las políticas de privacidad de una determinada página no hablen expresamente de la publicación de su información, siempre pueden existir vacíos o confusiones en los términos en que dicha política ha sido pensada y redactada, haciéndonos vulnerables ante posibles ataques.

Tomar medidas contra dicha problemática es a veces tan sencillo como minimizar los datos que lo pueden identificar ante terceros o llenar únicamente los espacios obligatorios en formularios de empresas de reconocida confianza.

Además de esto, se recomienda usar contraseñas de mínimo 14 caracteres, entre números, minúsculas y mayúsculas, una contraseña larga es fácil de recordar, pero difícil de descifrar para los demás. Se recomienda también no compartir contraseñas, incluso si es con personas de su entera confianza, así como evitar usar la misma contraseña en todas sus cuentas.

Evite pagar cuentas, realizar transacciones bancarias y hacer compras en una computadora pública o en cualquier dispositivo (como una computadora portátil o un teléfono celular) a través de una red inalámbrica pública.

VIII. CONCLUSIONES

El modelo de gestión de riesgos para la seguridad de la información establece cierto protocolo, que aplicado correctamente, ofrece un conocimiento a detalle de los problemas que podrían impedir el correcto funcionamiento de una organización y del cumplimiento de los objetivos primarios de ésta; dicho conocimiento es relevante, porque ofrece un planteamiento de medidas de control que resulte más fácil de aplicar, ya que el paneo general de una situación desde una óptica más elevada y detallada, permite afrontar un evento riesgoso para la seguridad informática.

En el campo de la gestión tecnológica en organizaciones como el Consejo Superior de la Judicatura, el modelo de riesgo implementa una interrelación de cada departamento de gestión, en dónde el área tecnológica está al servicio de los demás para brindar apoyo en el desarrollo de sus funciones. El modelo de gestión, más exactamente, el mapa de riesgos, ofrece precisamente un recurso para que en eventos que presuponen un peligro para la organización sean afrontados de la mejor manera, disminuyendo, en la medida de lo posible, un impacto mayor, que podría ser catastrófico para la organización, y en esta misma vía, para la administración de justicia en Colombia.

Es evidente que el usar herramientas como el de la nube, para guardar información de alta importancia, suponen gran desconfianza de cuán vulnerables pueden llegar a ser estos sistemas, por cuanto el exponer información en internet nos hace objeto de muchos riesgos ante terceros; pues bien, atendiendo a las anteriores sugerencias, tales como el cifrado de datos o un sistema de doble autentificación, y con una actitud de protección efectiva de nuestros datos, se puede hacer más efectiva la seguridad de la nube y en esta misma vía, la de nuestros datos.

La protección a la privacidad comienza por nosotros mismos, pues somos los principales responsables de administrar que tipo de información queremos almacenar en sistemas como el de la nube, y hacerlo de una manera segura es aún más una expresión de nuestra voluntad, pues entre más medidas y recomendaciones implementemos para fortalecerla, menos riesgos tendremos de perder información.

REFERENCIAS

[1] Iván López, Contraloría General Veracruz, "Guía de Aplicación del Modelo de Administración de Riesgos",[online],Disponible: http://sistemas.cgever.gob.mx/2013/normas_generales/GModelo%20de%20Admon%20de%20Riesgos.pdf

[2] Sala Administrativa, Autor Hernando Torres Corredor, "Sistema Integrado de Gestión Calidad,", (2010)

[3] Consejo Superior de la Judicatura, Mapa de procesos "Matriz de Riesgos",[online][intranet],Disponible: http://200.74.129.92/ModeloCSJ/portal/index.php?idcategoria=8

[4] Microsoft, "Centro de Seguridad y Protección",[online],Disponible: http://www.microsoft.com/es-xl/security/online-privacy/prevent.aspx

[5] Cristo Velasco San Martin, "Boletín Política Informática", [online] Disponible: http://www.inegi.org.mx/inegi/contenidos/espanol/prensa/contenidos/Articulos/tecnologia/libertad.pdf

Eliana Niño Cifuentes
Ingeniera de Sistemas. Universidad Incca de Colombia
Aspirante a Especialista en Seguridad Informática, Seminario de Investigación Aplicada, Universidad Piloto de Colombia